IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. No.:	10/028,874	Confirmation No.	**4659**
Applicant:	HEPWORTH et al.	TC/A.U.:	2152
Filed:	October 22, 2001	Examiner	Truong, L.
Docket No.:	4366-43	Confirmation No.:	4659
Customer No.:	*22442*		

For: "REAL TIME CONTROL PROTOCOL SESSION MATCHING"

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

The outstanding Final Office and Advisory Actions reject Claims 31-56 under 35 U.S.C.§103(a) as being unpatentable over Wan, et al., in view of Pruthi, et al., and further in view of Fuh, et al.

Appellants respectfully submit that the claims are allowable over the cited reference.

A common architecture for VoIP is to have a session monitor, in addition to each endpoint, to effect session management. To enable the monitor to obtain RTCP packets, a dual unicast architecture was developed. In dual unicast, one session participant (A) transmits both RTP and RTCP packets to the other session participant (B) and RTCP packets to the monitor. Dual unicast, however, exposes design limitations in the RTCP protocol itself. Although endpoint session ids are unique to a particular (first) session (such as between A and B), an endpoint in a concurrent (second) session (such as between C and D) can have the same session id or synchronization source id ("SSRC") as an endpoint (A or B) in the other (first) session. When duplicate endpoint session ids are concurrently in use, the monitor can have substantial difficulty determining which RTCP packets correspond to which session, potentially causing inaccurate performance analysis. This is so because the RTCP packets sent to the monitor include the address of only the source endpoint and exclude the address(es) of the other endpoint(s) to the session.

Independent claim 31 is directed to this problem. Step (a) describes the dual unicast architecture in which, during a first session, a first endpoint transmits first and second sets of packets, respectively, to a session monitor and second endpoint. The sets of packets contain differing information, with each packet in the first set being used for determining network performance information. When a packet in the first set is received by the session monitor, the monitor determines whether the packet corresponds to an active session entry recorded in a first set of data structures and, if so, updates the first data structure set. An active session entry in the first set of data structures has network addresses for each endpoint to a referenced active session. When the packet does not correspond to an active session entry, the monitor determines whether the packet corresponds to an active session entry in a second set of data structures and, if so, updates the second data structure set. Each entry in the second set of data structures fails to include a network address for each of the endpoints to a referenced active session. *See also* independent claim 40, the combination of independent claim 48 and dependent claim 50, and the combination of independent claims 51 and 53. Using the data structure sets and network address to define the session (rather than only session identifiers) can, after the startup interval, at least substantially eliminate misinterpretation of RTCP packets and incorrect analysis of performance data. The window of opportunity for possible confusion using the above algorithm(s) exists only when two different endpoints join different sessions at the same time and with the same session identifier.

In a dual unicast architecture, independent claim 48 is directed to the first endpoint receiving, from the second endpoint, a first packet comprising voice information and transmitting, in response, a second packet to a session monitor. The second packet includes the network addresses of *both* the first and second endpoints and is associated with the first packet set. Independent claim 54 is directed to a session packet for this architecture comprising a source network address of a participant to a VoIP session, a destination address of the session monitor, a network address of another session endpoint, and session information. Including in a session monitor packet the addresses of all of the session endpoints can greatly simplify packet matching with active session entries. *See also* independent claim 51.

Although Wan, et al., discloses a dual unicast architecture, Wan, et al., are silent regarding tracking active RTCP sessions to pair packetized performance information with the session.

Wan, et al., are directed to reducing congestion of real time data traffic on a multimedia communications network having a traffic control mechanism. Wan, et al., first extract from data traffic information regarding congestion of the network. This extraction is performed by a network of monitors receiving RTCP packets. A call admission control module in a central server regulates congestion by receiving, from the monitors, traffic information, using the information to analyze congestion status, and communicating instructions to the network to reduce congestion.

Pruthi, et al., teach packet sniffing rather than a dual unicast architecture and fail to address the use of differing sets of data structures to include entries for fully and partially identified active sessions.

In Pruthi, et al., a network monitor 102 extracts or "sniffs" packets from the bit stream on communication line 104 and converts them to records stored in memory. The records are generated by first determining the type (protocol or layer) of each packet (step 414) and then filtering the packets (step 416) based on their determined types. An index is generated (step 418) for each packet, and the packet is then converted into an indexed record (step 420). The time when the network monitor received each IP packet is used as an index for each IP packet. Exemplary information retained respecting each packet includes the type of the packet, the size of the packet, a packet number, source or destination address, an interface number, an application, and an associated session. Using the index, statistics measured include packet size distributions, protocol distributions, bandwidth usage per client, bandwidth usage by domain, average response time per server, average round-trip time between server-client pair, and performance metrics.

Fuh, et al., are directed to authentication and access control and teach nothing regarding dual unicast architectures let alone the use of differing sets of data structures to include entries for fully and partially identified active sessions.

In Fuh, et al., a network device is configured to intercept network traffic initiated from a client and directed toward a network resource and to locally authenticate the client. Authentication is carried out by comparing source IP address in the header against an Access Control List and, if

successful, searching authentication caches for the source IP address. When a corresponding cache is located, the client is authenticated. When a corresponding cache is not located, a linked authentication cache is created. If the source IP address does not match any of the ACL entries, the packet is denied passage.

None of the references teach (a) using the data structure sets and network address to identify VoIP sessions (rather than session identifiers alone) or (b) in a dual unicast architecture, an endpoint sending to the session monitor a packet including not only the source endpoint's network address but also the network address(es) of the other session participant endpoint(s).

In relevant part, the Examiner counters as follows:

(a) Wan, et al., teach, at col. 8, lines 6-19), the use of RTCP and therefore it would have been obvious based on Wan, et al., to have network performance report entries indexed via electronic address and associated session identifier. Applicant disagrees. RTCP, which is disclosed in Wan, et al., uses SSRC's from endpoints to match, to a common session, discrete packet streams from differing endpoints. The session monitors of Wan, et al., are not disclosed as using network addresses alone or a combination of network addresses and SSRC's to match discrete packet streams. Using SSRC's alone can still cause differing sessions having the same SSRC to be treated as the same session.

(b) Pruthi, et al., teach, at ¶¶ [0040], [0046]-[0048], and [0065]-[0066], matching newly received indices (which can include source or destination IP address) against previously stored indices. This argument is flawed. Pruthi, et al., is sniffing packets exchanged directly between two endpoints that, for a given session, will always include the same two IP addresses either as source or destination (depending upon the direction of packet flow). Thus, the two IP addresses will appear in the original index and in any subsequently generated index. In other words, there will be no set of data structures in which one of the IP addresses is unknown. In a dual unicast structure in contrast, differing endpoints (the packet sources) are *separately* sending packets related to the same session *to the same session monitor* (the packet destination). Thus, until the packet streams are matched, the session monitor knows, for each discrete packet stream, only the IP address of one of the endpoints.

(c) It would have been obvious over Pruthi, et al., to know that data packets should include the respective addresses of the first and second computers (*see* ¶¶ [0045]-[0047]). This argument too is flawed. Claims 48 and 51 require the first endpoint to receive a voice packet from the other endpoint and, in response, transmit *to the session monitor* a second packet including the network addresses of the other endpoints to the session. Pruthi, et al., sniffs packets exchanged between two endpoints. Neither endpoint addresses a packet to the network monitor 102.

(d) Finally, the Examiner argues that (a) using first and second data structure sets to identify unidentified and identified sessions and (b) dual unicasting in which separate packets are transmitted to the other endpoint and a performance monitor are not in the rejected claims. Applicant disagrees. Feature (a) is claimed in dependent claims 36, 37, 45, 50, and 53, and feature (b) is claimed in independent claims 31, 40, 48, and 51. Applicant notes "unidentified" means simply that the other endpoint(s) to a packet stream has not yet been identified while "identified" means that the other endpoint(s) to the packet stream has been identified, and that "dual unicast" refers to an endpoint sending packets to another session endpoint and a session monitor. Both concepts are clearly claimed in this application.

Remand of the case to the Examiner for a prompt Notice of Allowance is thus earnestly solicited.

A Request for a One-Month Extension of Time is filed herewith. The Notice of Appeal is therefore believed to be timely. Please credit any overpayment or debit any underpayment to Deposit Account 19-1970 and if an additional extension is required such extension is hereby petitioned.

Respectfully submitted,

SHERIDAN ROSS P.C.

By: Douglas Swartz

Douglas W. Swartz
Registration No. 37,739
1560 Broadway, Suite 1200
Denver, Colorado 80202-5141
(303) 863-9700

Date: July 27, 2007